(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－309214

(43)公開日　平成６年(1994)11月４日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/00	５３７　Ｚ	8944－5B		
	12/14	３２０　Ａ	9293－5B		

審査請求　未請求　請求項の数３　ＯＬ　（全　６　頁）

(21)出願番号　特願平5－94383

(22)出願日　平成５年(1993)４月21日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　吉　武　良
東京都府中市東芝町１　株式会社東芝府中工場内

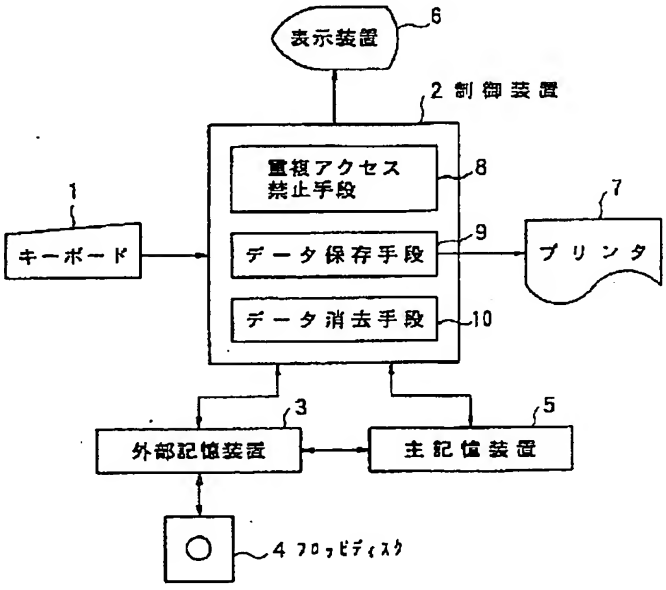
(74)代理人　弁理士　佐藤　一雄　（外３名）

(54)【発明の名称】　データベースシステム

(57)【要約】

【目的】　機密データについての保護機能を向上させる。

【構成】　ユーザは、自己の機密データについては自己のフロッピディスク４に記憶しておく。フロッピディスク４は、自己の手元に保管している限り、システムとは切り離されているので、他のユーザにシステムのラインを通じて機密データを知られたり、システム障害等によってデータの内容が破壊されたりすることはない。自己の機密データにアクセスする場合は、フロッピディスク４を外部記憶装置３にセットし、機密データを主記憶装置５の記憶領域に転送してデータ処理を行う。このとき、重複アクセス禁止手段８は、この記憶領域をロックし、他からのアクセスを禁止するので機密データが漏洩することはない。また、データ保存手段９は、アクセス終了後、記憶領域のデータをフロッピディスク４に書き込み、常に最新の機密データを保存しておく。データ消去手段１０は、記憶領域をクリアして、消し忘れによる機密データの漏洩を防止する。



【特許請求の範囲】
【請求項１】キーボード等の入力手段と、制御装置と、表示装置及びプリンタ等の出力手段と、主記憶装置と、データベースとして用いられる外部記憶装置とを備え、データのアクセスを行う場合は、入力手段からの情報に基づいて制御装置がアクセスを許可した後、外部記憶装置から取出したデータを主記憶装置の特定記憶領域へ移して行うデータベースシステムにおいて、
前記データベースのデータのうち機密データを記憶した外部記憶媒体を備えると共に、
前記制御装置は、前記主記憶装置の特定記憶領域に対する重複したアクセスを禁止する重複アクセス禁止手段を有しており、
機密データのアクセスを行う場合は、前記外部記憶媒体を外部記憶装置に装着し、この外部記憶媒体から取出した機密データを前記主記憶装置の特定記憶領域へ移すようにし、
しかも、一のユーザが機密データにアクセスしている場合は、他のユーザがこの機密データにアクセスできないようにしたことを特徴とするデータベースシステム。
【請求項２】請求項１記載のデータベースシステムにおいて、
前記制御装置は、
前記機密データのアクセス終了の際に、前記主記憶装置の特定記憶領域に格納されている機密データを、前記外部記憶装置に装着されている外部記憶媒体へ保存するデータ保存手段を有することを特徴とするデータベースシステム。
【請求項３】請求項１又は２記載のデータベースシステムにおいて、
前記制御装置は、
前記機密データのアクセス終了の際に、前記主記憶装置の特定記憶領域に格納されている機密データを消去するデータ消去手段を有することを特徴とするデータベースシステム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明はデータベースシステムに関するものであり、より詳しくは、データベースで扱うデータの中に機密データを含んでいるデータベースシステムに関するものである。
【０００２】
【従来の技術】近年、多方面でデータベースを利用したデータベースシステムが普及しており、データベースに含まれる情報を多くのユーザが利用できるようになっている。
【０００３】しかし、このような情報の中には、特定のユーザ以外には公開すべきでないものがある。例えば、個人のプライバシーに関する事項については、本人あるた、企業における人事情報等は、特定セクションあるいは特定人以外には知ることができないようにすべきであると考えるのが通常である。
【０００４】そのため、このように機密性が要求されるデータを扱うデータベースシステムにおいては、予め各ユーザ毎にユーザＩＤやパスワードを設定しておき、各ユーザがデータベースを利用しようとする場合には、これらユーザＩＤやパスワードが認識できたユーザのみに対して、データのアクセス権限を与えるようにしていた。
【０００５】
【発明が解決しようとする課題】ところが、このようなユーザＩＤやパスワードは、各ユーザの不注意や事故により、あるいは他人のスパイ的行為等により、その内容を第三者に知られてしまうことがある。
【０００６】このような場合、データベース中の機密データは、この第三者によってアクセスされてしまい、その機密データの正当利用者であるユーザや関係者は多大な損害を蒙むるおそれがある。
【０００７】また、データベースのデータは、一般に、外部記憶装置に備え付けられているハードディスク等に格納されているが、この外部記憶装置は、システム内の他の構成機器と常に電気的に接続可能になっているため、システム内に発生した事故や障害等によって、機密データが破壊されたり、アクセス不可能になるおそれがあった。
【０００８】本発明は、上記事情に鑑みてなされたものであり、機密データについての保護機能をより向上させることが可能なデータベースシステムを提供することを目的としている。
【０００９】
【課題を解決するための手段】上記課題を解決するための手段として、第１の発明は、キーボード等の入力手段と、制御装置と、表示装置及びプリンタ等の出力手段と、主記憶装置と、データベースとして用いられる外部記憶装置とを備え、データのアクセスを行う場合は、入力手段からの情報に基づいて制御装置がアクセスを許可した後、外部記憶装置から取出したデータを主記憶装置の特定記憶領域へ移して行うデータベースシステムにおいて、前記データベースのデータのうち機密データを記憶した外部記憶媒体を備えると共に、前記制御装置は、前記主記憶装置の特定記憶領域に対する重複したアクセスを禁止する重複アクセス禁止手段を有しており、機密データのアクセスを行う場合は、前記外部記憶媒体を外部記憶装置に装着し、この外部記憶媒体から取出した機密データを前記主記憶装置の特定記憶領域へ移すようにし、しかも、一のユーザが機密データにアクセスしている場合は、他のユーザがこの機密データにアクセスできないようにしたことを特徴とするものである。

て、前記制御装置は、前記機密データのアクセス終了の際に、前記主記憶装置の特定記憶領域に格納されている機密データを前記外部記憶装置に装着されている外部記憶媒体へ保存するデータ保存手段を有することを特徴とするものである。

【００１１】第３の発明は、第１又は第２記載のデータベースシステムにおいて、前記制御装置は、前記機密データのアクセス終了の際に、前記主記憶装置の特定記憶領域に格納されている機密データを消去するデータ消去手段を有することを特徴とするものである。

【００１２】

【作用】第１の発明の構成において、機密データについては、これを扱うユーザが予め決められており、各ユーザは自己の所有する外部記憶媒体に自己が扱うべき機密データを格納している。この外部記憶媒体は、常時は、各ユーザが自己の手元に置いておくものであり、システムとは切離された状態になっている。したがって、この機密データについては、他のユーザ等からアクセスされたり、システム障害等によりデータが破壊されたりすることはない。

【００１３】そして、ユーザが自己の外部記憶媒体に格納されている機密データにアクセスする場合は、この外部記憶媒体を外部記憶装置にセットする。次いで、この機密データ主記憶装置に移して、これを表示装置に表示したり、あるいはデータ内容を書換えたりする処理を行う。

【００１４】このように、機密データが主記憶装置に移されている間は、他のユーザからのアクセスにより機密データが漏洩されやすい状態になっている。しかし、重複アクセス禁止手段が、機密データが移されている特定記憶領域をロックし、他のユーザからのアクセスを禁止しているので、ユーザＩＤやパスワードを知られてしまったとしても、機密データが漏洩することはない。

【００１５】また、第２の発明によれば、機密データについて書換えを行った場合、その内容が自動的に外部記憶媒体に保存される。したがって、外部記憶媒体には常に最新の機密データが格納される。

【００１６】そして、第３の発明によれば、機密データのアクセス終了の際には、主記憶装置の特定記憶領域に格納されている機密データが自動的に消去される。したがって、ユーザの消し忘れによって、機密データが漏洩することはない。

【００１７】

【実施例】以下、本発明の実施例を図１乃至図３に基き説明する。図１は、本実施例に係るデータベースシステムの構成の一例を示すブロック図である。図１において、キーボード１からの信号が制御装置２に入力されると、制御装置２は、外部記憶装置３にセットされているフロッピディスク４のデータを主記憶装置５に転送するデータを表示装置６により表示したり、プリンタ７によりプリントアウトしたりする。この制御装置２は、図示するように、重複アクセス禁止手段８，データ保存手段９，データ消去手段１０を含んでいる。

【００１８】図２は、フロッピディスク４から転送されるデータを格納する、主記憶装置５内の記憶領域を示す説明図である。すなわち、ｎ人のユーザU_1，U_2，…，U_nがシステムに登録されているとすると、主記憶装置５内の記憶領域M_1，M_2，…，M_nもこれに対応してｎ個に分割されている。そして、各ユーザU_1，U_2，…，U_nの所有するフロッピディスク４のデータは、それぞれに割当てられた記憶領域に転送され、各ユーザは自己に割当てられた記憶領域に対してのみアクセスできるようになっている。

【００１９】次に、以上のように構成されるデータベースシステムの用い方を、図３のフローチャートを参照しつつ説明する。

【００２０】まず、各ユーザは自己の機密データについては、予め自己の所有するフロッピデイスク４に、その内容を書込んでおくようにする。なお、各ユーザのデータであって、機密にする必要のないものや、重要性の低いデータについては、従来通り、外部記憶装置３に備え付けられているハードディスクに記録しておくこととする。

【００２１】或るユーザ（例えばU_1とする。）が自己の所有するフロッピディスク４に書込まれた機密データにアクセスしようとする場合、ユーザU_1はこのフロッピディスク４を外部記憶装置３にセットし（ステップ１）、キーボード１等の入力手段によりユーザーＩＤやパスワードを制御装置２に入力させる（ステップ２）。制御装置２は、入力したこれらのユーザＩＤやパスワードが、予め登録されているものと一致するか否かを判別し、アクセス許可を与えるか否かについて決定する（ステップ３）。アクセス許可を与えないと決定した場合、制御装置２は、表示装置６の画面に、再入力を行うべき旨あるいはエラーの表示を行う。

【００２２】一方、アクセス許可を与えると決定した場合、制御装置２はログインし（ステップ４）、外部記憶装置３を回線に接続する。そして、制御装置２内の重複アクセス禁止手段８は、主記憶装置５の記憶領域において、ユーザU_1に割当てられた記憶領域M_1をロックし、他のユーザU_2～U_nからのアクセスを禁止する（ステップ５）。したがって、他のユーザU_2～U_nがたまたまユーザU_1のパスワード等を知っていたとしても、ユーザU_1のアクセス中にその機密データを盗むことは不可能となる。

【００２３】このように、記憶領域M_1が外部に対してロックされると、この記憶領域M_1に、フロッピディスク４の機密データが転送され、制御装置２はこのデータ

データは、データベース上の他のテーブルのデータと結合されるなどして、データ検索，変換，追加，削除等のデータ処理に用いられる（ステップ７）。

【００２４】このような機密データに対するデータ処理が終了すると、データ保存手段９は、主記憶装置５の記憶領域M_1に格納されている機密データを、外部記憶装置３にセットされているフロッピディスク４に保存する（ステップ８）。これにより、フロッピディスク４には常に最新の機密データを保存しておくことができる。

【００２５】次いで、データ消去手段１０は、記憶領域M_1をクリアし、記憶領域M_1に残っている機密データを消去する（ステップ９）。したがって、ユーザM_1が記憶領域の機密データを消し忘れることにより、アクセス終了後、他のユーザU_2～U_nに機密データが盗まれるのを防止することができる。

【００２６】記憶領域M_1がクリアされると、重複アクセス禁止手段８は、記憶領域M_1のロックを解除し（ステップ１０）、記憶領域M_1に対する再度のアクセスが可能な状態としておく。そして、制御装置２はログアウトを行い（ステップ１１）、ユーザU_1はフロッピディスク４を外部記憶装置３から取出す（ステップ１２）。

【００２７】上記した実施例では、ユーザU_1は、自己の機密データを自己の所有するフロッピディスク４に記録するようにしているので、ユーザU_1は、このフロッピディスク４を自己の手元に置いている限りは、システム上のラインを通じて他のユーザ等に機密データを知られるおそれは全くなく、また、システム障害等により機密データを破損されるおそれも全くない。

【００２８】システム上のラインを通じて機密データが漏洩するおそれがあるのは、ユーザU_1がフロッピディスク４を外部記憶装置３にセットし、自己の機密データにアクセスする場合であるが、この場合には、重複アクセス禁止手段８が記憶領域M_1をロックし、他のユーザ等からのアクセスを禁止しているので、この場合においても機密データが漏洩することはない。

【００２９】また、ユーザU_1が自己の機密データのデータ処理を終了した際は、データ保存手段９が記憶領域Ｍ１のデータをフロッピディスク４に書込むので、フロッピディスク４には常に最新の機密データが保存されていることになる。

【００３０】そして、データ消去手段１０は、機密データのデータ処理終了後は、記憶領域M_1のデータを消去するので、ユーザU_1がアクセス終了後にデータを消し忘れることによって機密データが漏洩するのを防止できる。

【００３１】なお、上記実施例では説明を簡単にするため、図１自体の構成をひとつのデータベースシステムとし、各ユーザU_1～U_nが自己の機密データにアクセスする場合は、各自が自己のフロッピディスク４を外部記憶装置３にセットすることを前提としていた。

【００３２】しかし、本発明のデータベースシステムは上記の態様に限られるわけではなく、例えば、図１に示された構成をシステム上の一つの端末コンピュータと考え（ホストコンピュータを別個に設けることとする。）、各ユーザU_1～U_nが自己専用の端末コンピュータを持っているものとしてもよい。

【００３３】また、上記実施例では、外部記憶媒体がフロッピディスクである場合について説明したが、もちろん、これに限られるわけではなく、磁気テープなどの他の媒体を使用することが可能である。

【００３４】

【発明の効果】以上のように、本発明によれば、常時はシステムと切り離して保管することができる外部記憶媒体に機密データを記録するようにし、この外部記憶媒体をシステムに接続して機密データにアクセスする場合は、重複アクセス禁止手段が主記憶装置の記憶領域を外部に対してロックする構成としているので、機密データについての保護機能を向上させることができる。

【図面の簡単な説明】

【図１】本発明の実施例の構成を示すブロック図。

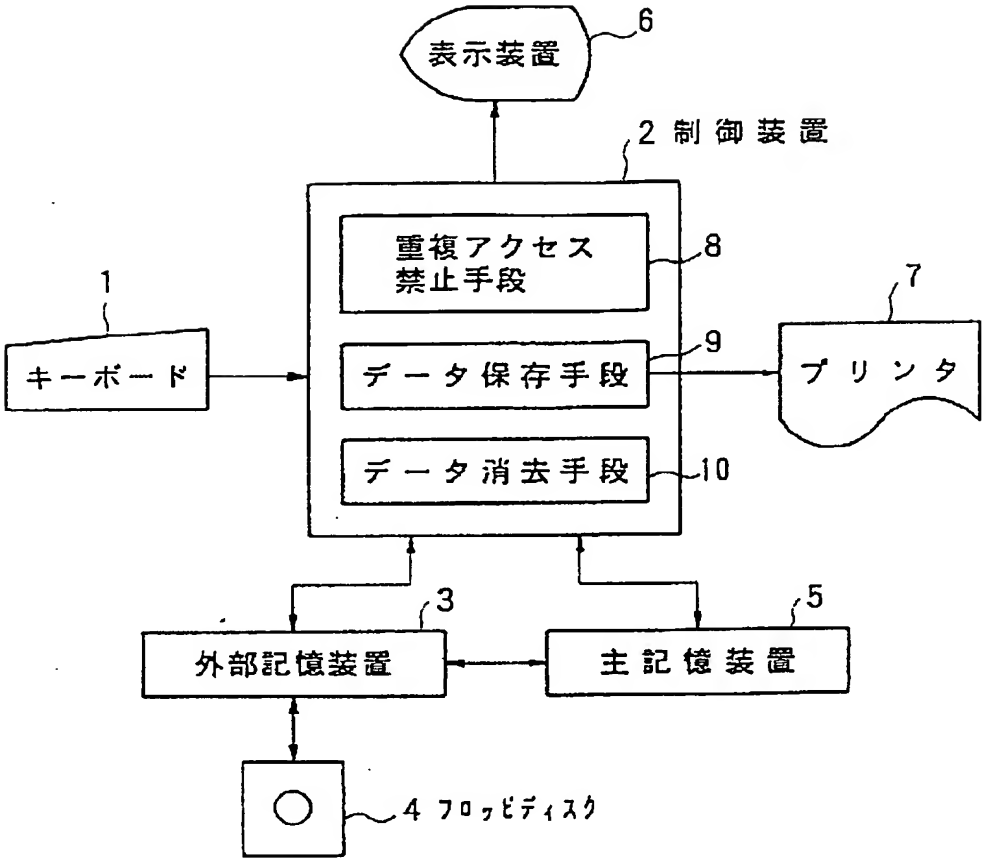
【図２】図１における主記憶装置内の記憶領域を示す説明図。

【図３】図１の動作を説明するためのフローチャート。

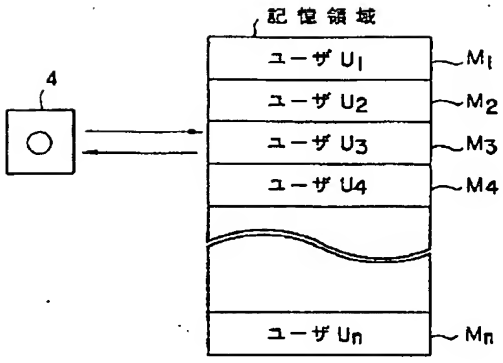
【符号の説明】

１　キーボード（入力手段）
２　制御装置
３　外部記憶装置
４　フロッピディスク（外部記憶媒体）
５　主記憶装置
６　表示装置（出力手段）
７　プリンタ（出力手段）
８　重複アクセス禁止手段
９　データ保存手段
１０　データ消去手段

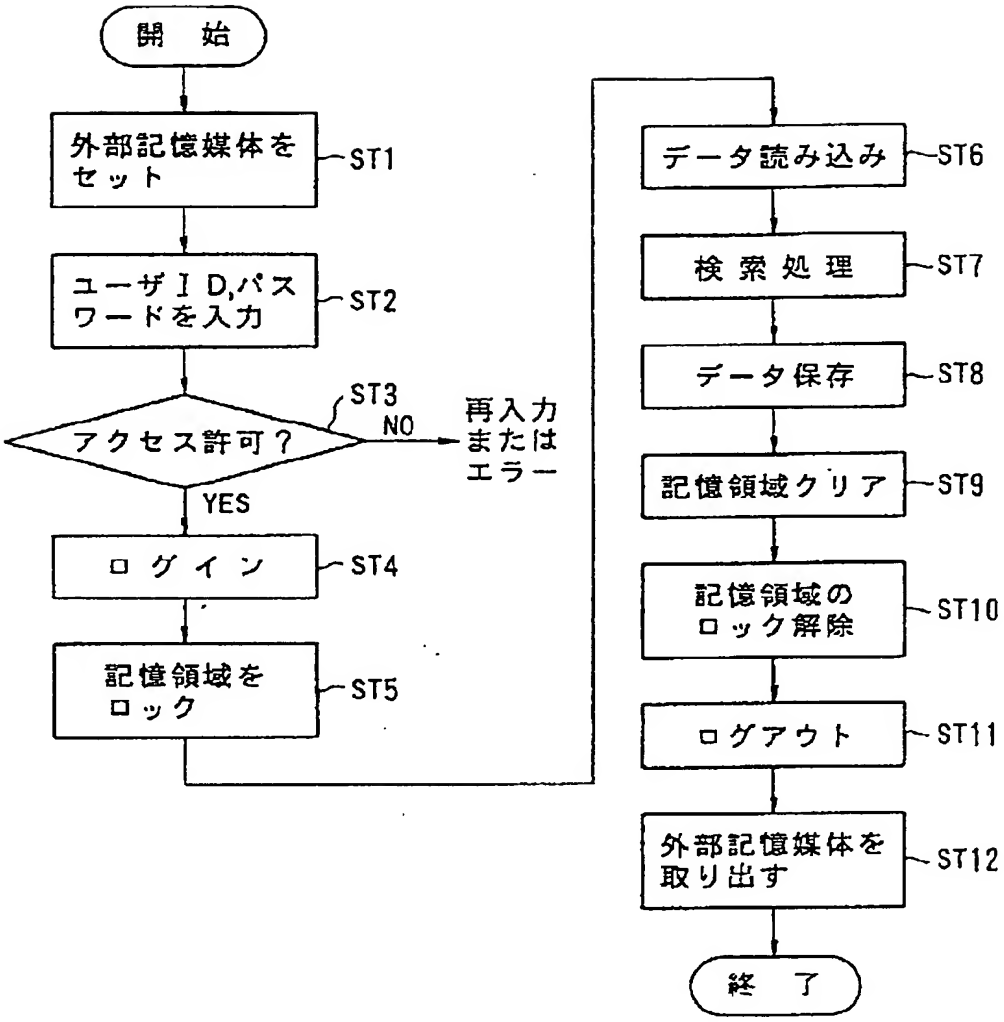
【図１】


表示装置
6
2 制御装置
重複アクセス
禁止手段
8
1
7
キーボード
9
データ保存手段
プリンタ
データ消去手段
10
3
5
外部記憶装置
主記憶装置
4 フロッピディスク

【図２】


記憶領域
4
ユーザ U1
M1
ユーザ U2
M2
ユーザ U3
M3
ユーザ U4
M4
ユーザ Un
Mn

【図３】


開　始
外部記憶媒体をセット
ST1
ユーザＩＤ,パスワードを入力
ST2
ST3
アクセス許可？
NO
再入力またはエラー
YES
ログイン
ST4
記憶領域をロック
ST5
データ読み込み
ST6
検索処理
ST7
データ保存
ST8
記憶領域クリア
ST9
記憶領域のロック解除
ST10
ログアウト
ST11
外部記憶媒体を取り出す
ST12
終　了